Claims

What is claimed is:

1. A computer-based method of constructing one or more correlation rules for use by an event management system for managing a network with one or more computing devices, the method comprising the steps of:

selecting one or more event patterns representing event data associated with the network of computing devices being managed by the event management system;

automatically learning predicates of the one or more correlation rules from the one or more selected event patterns; and

adding one or more corresponding actions to the one or more automatically learned predicates to form the one or more correlation rules.

2. The method of claim 1, further comprising the step of storing the one or more correlation rules in a rule database for access by the event management system.

3. The method of claim 1, wherein the event pattern selection step further comprises the step of a user marking the one or more event patterns in accordance with a data visualization of at least a portion of the event data.

4. The method of claim 1, wherein the event pattern selection step employs a data mining algorithm.

5. The method of claim 1, wherein the automatic predicate learning step comprises the steps of:

learning an initial concept;

determining if acceptance criteria are met given the event data;

querying historical event data for similar event patterns; and

allowing the user to edit the initial concept based on the historical event data query.

6. The method of claim 1, wherein the automatic predicate learning step utilizes one or more abstraction hierarchies.

7. The method of claim 6, wherein the one or more abstraction hierarchies comprise a hierarchy for at least one of a host and an event type.

8. Apparatus for constructing one or more correlation rules for use by an event management system for managing a network with one or more computing devices, the apparatus comprising:

at least one processor operative to: (i) permit selection of one or more event patterns representing event data associated with the network of computing devices being managed by the event management system; (ii) automatically learn predicates of the one or more correlation rules from the one or more selected event patterns; and (iii) add one or more corresponding actions to the one or more automatically learned predicates to form the one or more correlation rules; and

a memory, coupled to the at least one processor, which stores the one or more correlation rules for access by the event management system.

9. The apparatus of claim 8, wherein the event pattern selection operation further comprises a user marking the one or more event patterns in accordance with a data visualization of at least a portion of the event data.

10. The apparatus of claim 8, wherein the event pattern selection operation employs a data mining algorithm.

11. The apparatus of claim 8, wherein the automatic predicate learning operation further comprises: (i) learning an initial concept; (ii) determining if acceptance criteria are met given the event data; (iii) querying historical event data for similar event patterns; and (iv) allowing the user to edit the initial concept based on the historical event data query.

12. The apparatus of claim 8, wherein the automatic predicate learning operation utilizes one or more abstraction hierarchies.

13. The apparatus of claim 12, wherein the one or more abstraction hierarchies comprise a hierarchy for at least one of a host and an event type.

14. An article of manufacture for constructing one or more correlation rules for use by an event management system for managing a network with one or more computing devices, the article comprising a machine readable medium containing one or more programs which when executed implement at least one of the steps of:

selecting one or more event patterns representing event data associated with the network of computing devices being managed by the event management system;

automatically learning predicates of the one or more correlation rules from the one or more selected event patterns; and

adding one or more corresponding actions to the one or more automatically learned predicates to form the one or more correlation rules.

15. The article of claim 14, further comprising the step of storing the one or more correlation rules in a rule database for access by the event management system.

16. The article of claim 14, wherein the event pattern selection step further comprises the step of a user marking the one or more event patterns in accordance with a data visualization of at least a portion of the event data.

17. The article of claim 14, wherein the event pattern selection step employs a data mining algorithm.

18. The article of claim 14, wherein the automatic predicate learning step comprises the steps of:

learning an initial concept;

determining if acceptance criteria are met given the event data;

querying historical event data for similar event patterns; and

allowing the user to edit the initial concept based on the historical event data query.

19. The article of claim 14, wherein the automatic predicate learning step utilizes one or more abstraction hierarchies.

20. The article of claim 19, wherein the one or more abstraction hierarchies comprise a hierarchy for at least one of a host and an event type.